PCT/EP98/04424

BUNDESREPUBLIK DEUTSCHLAND

09/485408

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Bescheinigung

Herr Siegfried E. W i l h e l m in München/Deutschland und die Deutsche Telekom AG in Bonn/Deutschland haben eine Patentanmeldung unter der Bezeichnung

"Decoder-Einrichtung für die Entschlüsselung von verschlüsselten Fernseh-Programmen"

am 6. August 1997 beim Deutschen Patentamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig das Symbol H 04 N 7/167 der Internationalen Patentklassifikation erhalten.

München, den 25. Mai 1998
Der Präsident des Deutschen Patentamts
Im Auftrag

Hiebinger

nzeichen: 197 34 071.7

A 9161
6.90
(EDV-L)
01/98

Siegfried Wilhelm
Deutsche Telekom AG

Decoder-Einrichtung für die Entschlüsselung von verschlüsselten Fernseh-Programmen

Die Erfindung betrifft eine Decoder-Einrichtung für die Entschlüsselung von verschlüsselten Fernseh-Programmen. Insbesondere betrifft die Erfindung eine Decoder-Einrichtung mit einer Bedienungseinheit, für die Entschlüsselung von verschlüsselten Fernseh-Programmen, mit einem Eingang zum Einspeisen eines verschlüsselten Fernseh-Programmes, einer Entschlüsselungseinrichtung, die ein verschlüsseltes Fernseh-Programm in ein mittels eines Fernseh-Empfängers wiedergebbares Format entschlüsselt, einem Ausgang, der mit einem Fernseh-Empfänger verbindbar ist, um das entschlüsselte Fernseh-Programm in den Fernseh-Empfänger zur Wiedergabe einzuspeisen, einer Schnittstelle für ein Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung, und einer Schnittstelle für eine Bedienungseinheit der Decoder-Einrichtung.

Mit einer derartigen Decoder-Einrichtung ist der Empfang und die Entschlüsselung von sog. Pay-TV Programmen möglich, wobei derzeitige Decoder-Einrichtungen als sog. Set-Top-Boxen zu herkömmlichen Fernseh-Empfängern im Handel erhältlich sind.

Die bisher üblichen, zum Beispiel monatlichen Abrechnungen, für die Bereitstellung des Programms bei Pay-TV weichen mehr und mehr einer individuellen ("pay-per-view") Abrechnungs-Praxis. Daher besteht die Notwendigkeit einer Identifizierung und Authentifizierung des Programm-Kunden vor dem Zugriff des Programm-Kunden auf das Programm. Außerdem werden bei sog. HOT-Programmen (Home Order Television) auch Bestellungen des Programm-Kunden gegen dessen Bankkonto oder seine Guthaben auf einer Chip-Karte verrechnet. Auch hierbei sind Identifizierung und Authentifizierung des Programm-Kunden sowie ggf. Sicherungs-Mechanismen gegen Mißbrauch erforderlich.

Zur Sicherung elektronischer Abrechnungsverfahren sowie zum Schutz vertraulicher Informationen (Bankverbindungsdaten, Konto-Stand etc.) werden Chipkarten eingesetzt, die Microprozessoren haben, die mit Verschlüsselungsalorithmen ausgestattet sind. Ein derartiger Verschlüsselungsalorithmus ist der sog. RSA-Algorithmus. Beim Pay-TV ist eine derartige Chipkarte Teil des sog. "Conditional Access System" (CAS), mit der geprüft wird, ob der Anfragende tatsächlich der authorisierte Programm-Kunde ist, und ggf. ob seine Bonität für die gewünschte Leistung ausreicht. Auch bei sog. "Electronic Commerce" repräsentiert diese Chipkarte die Identität des Kunden bzw. seine elektronische Geldbörse. Dabei kann auf der Chipkarte ein Guthaben vermerkt sein, das aufgefüllt werden kann. Zugriffe auf die Chipkarte durch Dritte (Programm-Provider, Handel oder dergl. Erfolgen in der Regel durch mehr oder weniger automatisierten telefonischen oder Internet-Kontakt mit der Set-Top-Box vor oder bei der Transaktion.

Ein wachsendes Problem in diesem Zusammenhang ist die steigende Anzahl von Anbietern von Programmen oder Leistungen, die ein Programm-Kunde über diese Medien beziehen kann. Damit wird auch der Geräte-Aufwand (Set-Top-Box, Fernseh-Gerät, Internet-Endgerät (PC oder Net-PC), Fernbedienungsgeräte für die Set-Top-Box und das Fernseh-Gerät, sowie die Anzahl der für die Inanspruchnahme der einzelnen Dienste oder Leistungen notwendigen Chip-Karten immer größer.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, diese unterschiedlichen Komponenten preiswerter zu gestalten, das heißt ihren Hardware-Aufwand zu verringern, und diese unterschiedlichen Komponenten in der Handhabung für den Programm-Kunden einfacher und fehlerunanfälliger zu gestalten. Außerdem soll die Erfindung dem in steigendem Maß relevanten Problem der Sicherheit im Zusammenhang mit der Leistungs-Inanspruchnahme durch unbefugte Dritte Rechnung tragen.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, daß die Schnittstelle für das Identifikations- und/oder Schlüsselträgerbauteil in der Bedienungseinheit der Decoder-Einrichtung angeordnet ist.

Durch diese Ausgestaltung können Schnittstellen eingespart werden. Außerdem ist der Programm-Kunde (Benutzer) auf bequemere Weise in der Lage, seine Transaktionen auszuführen, da die Bedienungseinheit der Decoder-Einrichtung ohnehin mit einem Tastenfeld ausgestattet ist. Weiterhin erhöht sich die Sicherheit, da der Programm-Kunde (auch in größerem Kreis von Dritten seine Eingaben (PIN, TAN, etc.) tätigen kann, ohne daß dies von Dritten beobachtet werden kann. Außerdem kann die Bedienungseinheit der Decoder-Einrichtung zusammen mit dem Identifikations- und/oder Schlüsselträgerbauteil (= Chipkarte) sicher verwahrt werden, während in der Regel aus Bequemlichkeit eine Chipkarte nicht aus der Decoder-Einrichtung (= Set-Top-Box) entnommen wird.

Gemäß einer bevorzugten Ausführungsform der erfindungsgemäßen Decoder-Einrichtung mit einer Bedienungseinheit ist die Bedienungseinheit auch zur Bedienung des Fernseh-Empfänger-Gerätes eingerichtet, der eine Schnittstelle zum Empfang von Steuerbefehlen von der Bedienungseinheit aufweist. Dies reduziert den Geräte-Aufwand weiter. Außerdem kann damit auch der Zugriff auf das Fernseh-Empfänger-Gerät insgesamt kontrolliert werden. Das heißt, daß auch die Benutzung des Fernsehers für nicht zahlungspflichtige Programme nur bei Freigabe durch den authorisierten Benutzer möglich ist. Dies kann dadurch erreicht werden, daß die Funktion der Bedienungseinheit als Ganzes von der Eingabe der Kennung (PIN) des authorisierten Benutzer abhängt.

Insbesondere zur Abwicklung der Abbuchungen und zur Identifizierung und des Programm-Kunden durch der Programm-Anbieter dient bei der erfindungsgemäßen Decoder-Einrichtung eine Schnittstelle zu einem Telekommunikationsnetz. Dies kann ein MODEM sein. Oder für digitale Telekommunikationsnetze eine entsprechende Ankopplungseinrichtung sein.

Insbesondere zur Erhöhung der Sicherheit in dem System dient eine Schnittstelle zu einem Identifikations- und/oder Schlüsselträgerbauteil, durch das der Programm-Kunde über die oben beschriebene Schnittstelle zu einem Telekommunikationsnetz zu einem Dienste-Anbieter oder Waren-Versender Kontakt aufnehmen kann. Auch hier erfolgt die Herstellung einer Verbindung über das Telekommunikationsnetz mit einem bestimmten Teilnehmer (Dienste-Anbieter oder Waren-Versender) abhängig von einer Authorisierung durch das Identifikations- und/oder Schlüsselträgerbauteil erfolgt. Damit ist der Programm-Anbieter unabhängig von dem Dienste-Anbieter oder Waren-Versender in der Abrechnung mit dem Programm-Kunden. Dies kann Vorteile hinsichtlich der Datensicherheit und der Flexibilität mit sich bringen.

Alternativ dazu ist es jedoch auch möglich, daß der Programm-Anbieter mit dem Dienste-Anbieter eine geeignete Kooperation hat, so daß eine gemeinsame Abrechnung bzw. Kunden-Verwaltung und damit auch Kunden-Identifizierung und Kunden-Authorisierung erfolgen kann. In diesem Fall sind keine getrennten Chip-Karten erforderlich.

Unabhängig davon ist es vorteilhaft, wenn auch die Schnittstelle zu dem Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz in der Bedienungseinheit angeordnet ist.

Wie bereits erwähnt können das Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz und das Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung entweder durch zwei getrennte oder durch eine gemeinsame Chip-Karte realisiert sein.

In einer weiteren Ausgestaltung weist die Decoder-Einrichtung eine Schnittstelle auf, über die die Decoder-Einrichtung mit einem Rechner verbindbar ist, der zur Steuerung der Decoder-Einrichtung und/oder zur Herstellung einer Verbindung mit einem anderen Teilnehmer über das Telekommuni-

kationsnetz eingerichtet ist. Damit ist es möglich, die gesamten Funktionalität eines Rechners (PC oder Internet-PC), also die Speicherung und Verarbeitung von Daten und Informationen, sowie die komfortablere Gestaltung von Dialogen des Programm-Kunden mit zum Beispiel dem Programm-Anbieter oder dem Dienste-Anbieter für den Programm-Kunden verfügbar zu machen.

In einer besonders bevorzugten Ausführungsform der Erfindung ist die Bedienungseinheit durch den Rechner gebildet ist, der eine Schnittstelle aufweist, um die Decoder-Einrichtung zu steuern, und eine Schnittstelle für das Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz bzw. das Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung aufweist. Damit wird die Bereitstellung einer bzw. zwei separaten Bedienungseinheiten überflüssig. Es versteht sich, daß auch bei dieser Ausführungsform die beiden Chip-Karten für den Verkehr mit dem Programm-Anbieter und dem Dienste-Anbieter auch als eine gemeinsame Chip-Karte realisiert sein können.

Im übrigen kann die Verbindung zwischen dem Rechner und dem Fernseh-Gerät bzw. dem Rechner und der Decoder-Einrichtung sowohl drahtlos (zum Beispiel als Infrarot- oder als Ultraschallverbindung), als auch drahtgebunden sein kann. Außerdem kann der Rechner wegen seiner speziellen Anforderungen (relativ geringer Speicherbedarf, geringe Anforderungen an den Tastaturkomfort wegen der üblicherweise nur kurzen Eingaben etc.) auch als sog. Palmtop-Rechner ausgestaltet sein, der mit entsprechenden Schnittstellen (Infrarot-Schnittstelle zu der Decodier-Einrichtung so einer oder mehreren Schnittstellen für die Chip-Karte(n). Damit hat der Benutzer eine sehr kompakte und komfortable Steuerungs- und Bedienmöglichkeit seiner Geräte, aber auch die einfache Möglichkeit, mit dem Programm-Anbieter und/oder dem Dienste/Waren-Anbieter auf komfortable Weise zu kommunizieren. Schließlich verringert sich auch der Verkabelungsaufwand

zwischen den einzelnen Komponenten auf der Benutzerseite erheblich, was ebenfalls den Komfort erhöht.

Gemäß einer besonders bevorzugten Ausführungsform der Erfindung ist die Decoder-Einrichtung in das Fernsehgerät integriert. Damit wird dem Benutzer ein geschlossenes und gegen Mißbrauch besonders geschütztes Gerät zur Verfügung gestellt, bei dem alle Funktionen (herkömmliches Fernsehen, Pay-TV, Kommunikation mit einem Dienste/Waren-Anbieter über das Telekommunikationsnetz, Speicherung und/oder Nachbearbeitung der empfangenen Daten in dem Rechner etc.) in einer gegen Mißbrauch geschützten Weise ausführbar sind.

Die Erfindung betrifft auch eine Chip-Karte für eine vorstehend beschriebene Decoder-Einrichtung mit einer Bedienungseinheit, mit einer Rechnereinheit, einem ersten Speicherbereich, in dem zumindest Teile von Betriebssystem-Funktionen abgelegt sind, mit denen die Kommunikation zwischen der Rechnereinheit der Chip-Karte und den Peripherie-Geräten der Chip-Karte, sowie die Kommunikation mit einem externen Host-Rechner gesteuert wird, und mit denen geschützte, ungeschützte, und/oder Schreib/Lese-Speicher-Bereiche der Chip-Karte verwaltet werden, und einem zweiten Speicherbereich, der in geschützte und ungeschützte Bereiche unterteilt ist, wobei der Zugriff auf geschützte Bereiche in Abhängigkeit von einem Ergebnis einer Überprüfung der Zulässigkeit des Zugriffs erfolgt, wobei in dem geschützten Bereich des zweiten Speicherbereiches ein Generalschlüssel abgelegt ist, unter dessen Kontrolle die Eintragung wenigstens eines weiteren einfachen Schlüssels sowie eines zu diesem weiteren einfachen Schlüssel gehörendes Protokoll-Programm durch den externen Host-Rechner erfolgt.

Mit dieser Chip-Karte kann die vorstehend beschriebene Decoder-Einrichtung besonders sicher betrieben und auch einfach um den Zugriff auf mehrere weitere Dienste-Anbieter erweitert werden.

Vorzugsweise ist in dem zweiten Speicherbereich eine Schlüssel-Verwaltung abgelegt, von der aus der Zugriff auf ein Protokoll-Programm eines einfachen Schlüssels erfolgt.

Zur Ergänzung zusätzlicher Schlüssel bzw. Zugriffsmöglichkeiten auf weitere Anbieter dient dabei folgendes erfindungsgemäße Verfahren:
- Herstellen einer Telekommunikationsverbindung zwischen dem Host-Rechner und der Decoder-Einrichtung mit der Bedienungseinheit oder dem die Bedienungseinheit enthaltenden Rechner durch den Host-Rechner,
- Überprüfen des Generalschlüssels in der Chip-Karte durch den Host-Rechner,
- Übermitteln eines einfachen Schlüssels sowie eines zu diesem Schlüssel gehörenden Protokoll-Programmes an die Chip-Karte in verschlüsselter Form, falls die Überprüfung positiv ausfällt,
- Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in den geschützten Speicherbereich der Chip-Karte,
- Sperren des geschützten Speicherbereiches der Chip-Karte.

Dabei kann vor dem Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in den geschützten Speicherbereich der Chip-Karte der Schlüssel und das Protokoll-Programm durch die Rechnereinheit der Chipkarte entschlüsselt werden.

Fig. 1 zeigt eine Anordnung gemäß dem Stand der Technik in einem schematischen Blockdiagramm.

Fig. 2 - 4 zeigen unterschiedliche Ausführungsformen der vorliegenden Erfindung, jeweils in einem schematischen Blockdiagramm.

Fig. 1 zeigt eine derzeit übliche Endgeräteumgebung für kombinierte Pay TV- und Electronic-Commerce Anwendungen.

Über die Leitung (1) wird das breitbandige digital verschlüsselte Pay TV Nutzsignal durch das Fernseh-Gerät empfangen und über den Ausgang (4) an den Eingang (IN) in die Set-Top-Box (STB) übergeben. Dort wird das Signal von einem speziellen Chip mit einem hierfür vorgesehenen Algorithmus - der DVB-Algorithmus sei hier stellvertretend für alle genannt - entschlüsselt und an das Fernseh-Gerät zurückgegeben. Die Einstellung der Schlüssel erfolgt mittels einer Chipkarte (ICC DVB) über die Schnittstelle (3). Die Chipkarte enthält den Schlüsselverteilalgorithmus des Conditional Access Systems (z. B. RSA) und den geheimen Schlüssel des Kunden. Nur ein Kunde mit gültiger Chipkarte (ICC DVR) kann Pay TV Sendungen entschlüsseln. Die Chipkarte (ICC DVR) ist über die Chipkarten-Schnittstelle "IFD" an die Set-Top-Box (STB) angeschlossen.

Erweiterungen der Set-Top-Box (STB) sehen vor, daß ein Rückkanal über das Telefonnetz bzw. Internet über die Schnittstelle (5) mit den Servern verschiedener Dienstleistungsanbieter verbunden werden kann, um z.B. Dienstleistungen oder Artikel zu bestellen, die als Angebot in der Werbung der Pay TV Kanäle enthalten sind. Zur Sicherung von Bestellung und Bezahlung kann hier eine zweite Chipkarte (ICC BC) über eine weitere Schnittstelle (IFD) eingesteckt werden, so daß die Verbindung (6) zwischen der zweiten Chipkarte (ICC BC) und der weiteren Schnittstelle (IFD) hergestellt ist.

Weitere Anschlußmöglichkeiten der Set-Top-Box (STB) sehen die Verwendung einer IR-Fernbedienung (9) und eines Rechners PC über eine im PC-Umfeld übliche Schnittstelle (7), hier vereinfachend "PCI" genannt (z.B. V24/RS232C oder parallele Schnittstelle), vor. Mit dem Rechner PC lassen sich z.B. Rückkanalgeschäfte komfortabel gestalten oder Informationen aus den Pay TV Kanälen nachverarbeiten.

Zum Anschluß zweier Chipkarten an die Set-Top-Box (STB) gibt es verschiedene Lösungen. Entweder werden die Chipkartenterminals (IFD) fest in die Set-Top-Box (STB) einge-

baut oder sie werden steckbar als PCMCIA-Module ausgeführt. Mit Hilfe der PCMCIA Module entsteht die Möglichkeit, verschiedene Pay TV Zugangsverfahren (CAS) ohne Eingriffe in die Set-Top-Box (STB) gegeneinander auszuwechseln.

Nachteile der herkömmlichen Endgeräte-Konfiguration sind die geringe Bedienungsfreundlichkeit, die umständliche Verkabelung der Set-Top-Box (STB) und deren aufwendige Schnittstellengestaltung.

Die Fig. 2, 3 und 4 illustrieren Ausführungsformen der Erfindung.

Bereits in einer ersten Integrationsstufe nach Fig. 2 werden die Fernbedienungen von Set-Top-Box (STB) und Fernseh-Gerät (TV Set) in einem Gerät, der Bedienungseinheit (RCU) zusammengefaßt. Die neue Bedienungseinheit (RCU) erhält eine Chipkartenschnittstelle, die sowohl die Chipkarte (ICC DVB) des Pay TV Systems als auch die Chipkarte (ICC BC) des Rückkanals ansteuern kann. Der Schlüsselaustausch des Conditional Access Systems CAS des PAY TV geschieht zwar vom Ablauf her genauso wie in der herkömmlichen Konfiguration.

In Fig. 2 ist die Chip-Karte (ICC) DVB jedoch über die Bedienungseinheit (RCU) durch eine IR-Schnittstelle mit dem Pay TV Entschlüsselungschip (z. B. DVB) in der Set-Top-Box (STB) verbunden. Das Gleiche gilt für die Chip-Karte (ICC) BC, welche die Sicherung des Rückkanals nunmehr ebenfalls über die Bedienungseinheit (RCU) und deren IR-Schnittstelle vornimmt.

Damit entfällt das Einstecken der Chipkarten in die Set-Top-Box (STB) und somit auch alle Chipkartenschnittstellen an der Set-Top-Box (STB). Der Kunde steckt seine Karten direkt in die Fernbedienung RCU. Falls Pay-TV-Anbieter und Rückkanal-Dienstleister entsprechende vertragliche Vereinbarungen treffen, können die Funktionen beider Chipkarten ICC DVB und ICC BC sogar auf einer einzigen Chip-Karte (ICC) zusammengefaßt werden.

Der Rechner PC wird in Fig. 2ff entweder weiterhin über eine herkömmliche Schnittstelle (PCI) mit der Set-Top-Box (STB) verbunden oder nutzt hierzu ebenfalls die IR-Schnittstelle (Infra-Rot-Schnittstelle) der Set-Top-Box (STB).

Die Rückkanalanbindung an das Telekommunikationsnetz erfolgt entweder über die Set-Top-Box (STB) oder über den Rechner (PC). Grundsätzlich sind beide Varianten möglich.

Fig. 3 zeigt die Kombination von Fernbedienung (RCU) und dem Rechner (PC) in einer weiteren Integrationsstufe. Hierbei lassen sich die Vorteile des Rechners PC und der Fernbedienung (RCU) gleichzeitig nutzen. Diese Lösung wird insbesondere interessant, wenn es sich bei dem kombinierten Gerät RCU/PC um ein "Netzwerk-PC"-ähnliches Gerät handelt, welches kompakt und ohne aufwendige Peripherie und Verkabelung z.B. vom Wohnzimmertisch aus bedient werden kann.

In Fig. 4 ist die Vereinigung von Fernseh-Gerät (TV Set) und Set-Top-Box (STB) in nur einem Endgerät als eine weitere Integrationsstufe dargestellt.

Die in den Fig. 2 bis 4 dargestellten neuen Endgeräte-Konfigurationen zeigen, wie sich die Bedienung und die Verkabelung der Endgeräte nennenswert vereinfachen läßt ohne die Funktionalität zu beeinträchtigen.

Erfindungsgemäß werden also anstelle einer oder mehrerer Chipkartenschnittstellen an der Set-Top-Box (STB) nunmehr die betreffenden Chipkarten über eine Fernbedienung RCU und deren Infrarot-Schnittstellen mit dem in der Set-Top-Box (STB) verbleibenden Pay TV Entschlüsselungschip verbunden. Damit können aufwendige und anfällige Schnittstellen an der Set-Top-Box (STB) entfallen.

Außerdem können die Funktionen der Pay TV Chipkarte und der Rückkanal Chipkarte unter Zuhilfenahme einer speziellen

Fernbedienung RCU auf nur einer Karte bedienungsfreundlich kombiniert werden.

Schließlich ist durch die Kombination von Fernbedienung und PC in nur einem Gerät RCU/PC eine Verlagerung der Rückkanalanbindung aus der Set-Top-Box (STB) heraus ermöglicht. Damit ist eine optimale Nutzung des Internet PC (= PC, der über beliebige Online-Netze mit Servern von beliebigen Diensteanbietern verbunden ist), in Verbindung mit Pay TV Diensten einschließlich ihrer Rückkanaloptionen ermöglicht.

Ein weiterer Gesichtspunkt der Erfindung ist die Ausgestaltung der Chip-Karte, damit diese auch in der Lage ist, mit hohem Sicherheits-Niveau sowohl die Programm-Entschlüsselung des Programms des Pay-TV-Anbieters, als auch die Transaktion (Bestellung und Kaufpreis-Entrichtung) bei dem Waren/Dienstleistungs-Anbieter abzuwickeln.

Insbesondere, wenn im Laufe der Zeit weitere Waren/Dienstleistungs-Anbieter dazukommen, hätte dies zur Folge, daß der Programm-Kunde jeweils eine neue Chip-Karte benötigt, die die Schlüssel und Protokolle der bisherigen Anbieter (sowohl Pay-TV-Anbieter, als auch Waren/Dienstleistungs-Anbieter) enthält, als auch den Schlüssel und das Protokoll des neu dazugekommenen.

Hierfür bietet die Erfindung ebenfalls eine Lösung:
Da der Waren/Dienstleistungs-Anbieter ohnehin in der Regel durch den gleichen Host-Rechner mit dem Benutzer in Verbindung tritt wie der Pay-TV-Anbieter, kann dieser Host auch über einen Generalschlüssel auf die gesperrten Bereiche der Chip-Karte des Kunden zugreifen, um dort einen weiteren Schlüssel und das zugehörige Protokoll für zukünftige Transaktionen (Entschlüsselungs- oder Zahlungsvorgänge) abzulegen.

Außerdem ist in einem weiteren (ggf. ebenfalls gesperrten) Bereich eine Vektorentabelle oder eine Abfrage-Routine zu führen, in der nacheinander die neu dazukommenden Schlüssel

verwaltet werden. Beim Zugriff auf die Chipkarte wird zunächst anhand der Vektorentabelle oder der Abfrage-Routine geprüft, ob ein passender Schlüssel vorhanden ist, bzw. ob der durch den Benutzer eingegebene Schlüssel mit einem der auf der Chip-Karte abgelegten Schlüssel zusammenpaßt. Erst wenn das Ergebnis dieser Abfrage positiv ist, wird das zu dem jeweiligen Schlüssel gehörige Programm zur Transaktion bzw. Entschlüsselung (ggf. entschlüsselt und dann) ausgeführt.

Vorzugsweise wird der Schlüssel und das zugehörige Protokoll(-Programm) in ebenfalls verschlüsselter Form von dem Host-Rechner an die Set-Top-Box (STB) übertragen, und von dort über die Schnittstelle an die Bedienungseinheit (RCU) weitergegeben. Falls die Bedienungseinheit (RCU) in den Rechner (PC/RCU) integriert ist, kann der Host-Rechner Rechner direkt über das Telekommunikationsnetz mit dem Rechner (PC/RCU) in Verbindung treten, um die Informationenen für die bzw. in die Chip-Karte (ICC) zu übertragen.

Je nach konkreter Ausgestaltung kann das Protokoll(-Programm) in der Chip-Karte nur in verschlüsselter Form abgelegt sein, und jeweils zur Laufzeit vor der Ausführung entschlüsselt werden. Alternativ dazu kann das Protokoll(-Programm) jedoch auch beim Ablegen in dem (geschützten) Speicherbereich der Chipkarte in eine lauffähige Form gebracht werden.

Damit enthält der Speicher der Chip-Karte (neben anderem) folgende Programme bzw. Daten:

Einen Betriebssystem-Kern, mit dem die Kommunikation zwischen dem Prozessor der Chip-Karte und den Peripherie-Geräten auf der Chip-Karte, sowie die Kommunikation mit dem Host-Rechner gesteuert wird, der die Speicherbereiche der Chip-Karte (geschützte und ungeschützte Bereiche, Schreib/Lese-Bereiche, Flash-EEPROM etc.) verwaltet usw.

Schlüssel (ein Haupt- oder General-Schlüssel, sowie ein oder mehrere Anwendungs-Schlüssel), wobei der Haupt-Schlüssel dazu dient, (weitere) Anwendungs-Schlüssel und die zugehörigen Anwendungs- oder Protokoll-Programme in den Speicher-Bereich zu transferrieren. Die Anwendungs-Schlüssel dienen dazu sicherzustellen, daß die Ausführung der Protokoll-Programme (und damit der Abwicklung von Bestellungen oder die Entschlüsslung von Pay-TV-Programmen) nur bei Vorliegen der richtigen Eingabe durch den Benutzer erfolgt.

Verschlüsselte Anwender-Programme oder Protokoll-Programme, mit denen die Abwicklung von Bestellungen oder die Entschlüsselung von Pay-TV-Programmen gesteuert wird.

Zur weiteren Erhöhung der Sicherheit ist es vorgesehen, die Identifizierung und Authentifizierung zwischen der Bedienungseinheit (RCU) und/oder der Set-Top-Box (STB) bzw. Fernseh-Gerät (TV Set) einerseites und dem Host-Rechner andererseits auf unterschiedlichen Wegen bzw. Kanälen durchzuführen. Mit anderen Worten werden ein Teil des Protokollverkehrs über die Schnittstelle (5) zum Telefon-Netz und ein weiterer Teil über die Leitung (1) mit oder vor dem breitbandigen digital verschlüsselten Pay TV Nutzsignal übertragen. Dabei kann auch die Freischaltung/Sperrung von Diensten auf diesen Wegen erfolgen. Da für einen Mißbrauch dann beide Kanäle synchron abzuhören und zu entschlüsseln wären, ist so die Sicherheit erheblich höher. Insbesondere ist es möglich, die Informationen mit der Freischaltung/ Sperrung oder neue Schlüssel etc. auf die beiden Kanäle so zu verteilen, daß sie nur wechselweise und auch nur stufenweise in jeweiliger Kenntnis entschlüsselt werden können.

Ansprüche

1. Decoder-Einrichtung mit einer Bedienungseinheit (RCU), für die Entschlüsselung von verschlüsselten Fernseh-Programmen, mit
- einem Eingang (4) zum Einspeisen eines verschlüsselten Fernseh-Programmes,
- einer Entschlüsselungseinrichtung (DVB), die ein verschlüsseltes Fernseh-Programm in ein mittels eines Fernseh-Empfängers (TV Set) wiedergebbares Format entschlüsselt,
- einem Ausgang (2), der mit einem Fernseh-Empfänger (TV Set) verbindbar ist, um das entschlüsselte Fernseh-Programm in den Fernseh-Empfänger (TV Set) zur Wiedergabe einzuspeisen,
- einer Schnittstelle (IFD 3,6) für ein Identifikations- und/oder Schlüsselträgerbauteil (ICC DVB) zur Freigabe des Entschlüsselungseinrichtung (DVB), und
- einer Schnittstelle (IR 3,6) für eine Bedienungseinheit (RCU) der Decoder-Einrichtung (DVB),
dadurch gekennzeichnet, daß
- die Schnittstelle (IFD 3,6) für das Identifikations- und/oder Schlüsselträgerbauteil (ICC DVB) in der Bedienungseinheit (RCu) der Decoder-Einrichtung (STB) angeordnet ist.

2. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach Anspruch 1, dadurch gekennzeichnet, daß
- die Bedienungseinheit (RCU) auch zur Bedienung des Fernseh-Empfängers (TV Set) eingerichtet ist, der eine Schnittstelle (IR (,9) zum Empfang von Steuerbefehlen aufweist.

3. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach Anspruch 1, gekennzeichnet durch
- eine Schnittstelle (BC 5) zu einem Telekommunikationsnetz.

4. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach Anspruch 3, gekennzeichnet durch
- eine Schnittstelle (IFD 3,6) zu einem Identifikations- und/oder Schlüsselträgerbauteil (ICC BC), wobei die Herstellung einer Verbindung über das Telekommunikationsnetz mit einem bestimmten Teilnehmer abhängig von einer Authorisierung durch das Identifikations- und/oder Schlüsselträgerbauteil (ICC BC) erfolgt.

5. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Schnittstelle zu dem Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz in der Bedienungseinheit (RCU) angeordnet ist.

6. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- das Identifikations- und/oder Schlüsselträgerbauteil für die Authorisierung der Verbindung über das Telekommunikationsnetz und das Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung entweder durch zwei getrennte oder durch eine gemeinsame Chip-Karte realisiert sind.

7. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Decoder-Einrichtung eine Schnittstelle (DVB) aufweist über die die Decoder-Einrichtung mit einem Rechner (PC) verbindbar ist, der zur Steuerung der Decoder-Einrichtung und/oder zur Herstellung einer Verbindung mit einem anderen Teilnehmer über das Telekommunikationsnetz eingerichtet ist.

8. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Bedienungseinheit (RCU) durch den Rechner (PC) gebildet ist, der
- eine Schnittstelle (IR 3,7) aufweist, um die Decoder-Einrichtung zu steuern, und
- eine Schnittstelle (IFD 3,6) für das Identifikations- und/oder Schlüsselträgerbauteil (ICC BC) für die Authorisierung der Verbindung über das Telekommunikationsnetz bzw. das Identifikations- und/oder Schlüsselträgerbauteil (ICC DVB) zur Freigabe des Entschlüsselungseinrichtung (DVB) aufweist.

9. Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß
- die Decoder-Einrichtung in das Fernsehgerät integriert ist.

10. Chip-Karte für eine Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der vorhergehenden Ansprüche, mit
- einer Rechnereinheit,
- einem ersten Speicherbereich, in dem zumindest Teile von Betriebssystem-Funktionen abgelegt sind, mit denen die Kommunikation zwischen der Rechnereinheit der Chip-Karte und den Peripherie-Geräten der Chip-Karte, sowie die Kommunikation mit einem externen Host-Rechner gesteuert wird, und mit denen geschützte, ungeschützte, und/oder Schreib/Lese-Speicher-Bereiche der Chip-Karte verwaltet werden, und
- einem zweiten Speicherbereich, der in geschützte und ungeschützte Bereiche unterteilt ist, wobei der Zugriff auf geschützte Bereiche in Abhängigkeit von einem Ergebnis einer Überprüfung der Zulässigkeit des Zugriffs erfolgt, dadurch gekennzeichnet, daß
- in dem geschützten Bereich des zweiten Speicherbereiches ein Generalschlüssel abgelegt ist, unter dessen Kontrolle die Eintragung wenigstens eines weiteren einfachen Schlüs-

sels sowie eines zu diesem weiteren einfachen Schlüssel gehörendes Protokoll-Programm durch den externen Host-Rechner erfolgt.

11. Chip-Karte nach Anspruch 10, dadurch gekennzeichnet, daß
- in dem zweiten Speicherbereich eine Schlüssel-Verwaltung abgelegt ist, von der aus der Zugriff auf ein Protokoll-Programm eines einfachen Schlüssels erfolgt.

12. Verfahren zur Kommunikation eines Host-Rechners eines Pay-TV-Anbieters mit einer Decoder-Einrichtung mit einer Bedienungseinheit (RCU) nach einem der Ansprüche 1 - 9, und einer Chip-Karte nach einem der Ansprüche 10, 12 gekennzeichnet durch folgende Schritte:
- Herstellen einer Telekommunikationsverbindung zwischen dem Host-Rechner und der Decoder-Einrichtung mit der Bedienungseinheit oder dem die Bedienungseinheit enthaltenden Rechner durch den Host-Rechner,
- Überprüfen des Generalschlüssels in der Chip-Karte durch den Host-Rechner,
- Übermitteln eines einfachen Schlüssels sowie eines zu diesem Schlüssel gehörenden Protokoll-Programmes an die Chip-Karte in verschlüsselter Form, falls die Überprüfung positiv ausfällt,
- Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in den geschützten Speicherbereich der Chip-Karte,
- Sperren des geschützten Speicherbereiches der Chip-Karte.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß
- vor dem Eintragen des einfachen Schlüssels sowie des zu diesem Schlüssel gehörenden Protokoll-Programmes in den geschützten Speicherbereich der Chip-Karte der Schlüssel und das Protokoll-Programm vorzugsweise durch die Rechnereinheit der Chipkarte entschlüsselt werden.

14. Verfahren nach Anspruch 12, dadurch gekennzeichnet, daß ein Teil des Datenübertragungsverkehrs über die

Schnittstelle (5) zum Telefon-Netz und ein weiterer Teil über die Leitung (1) mit oder vor dem breitbandigen digital verschlüsselten Pay TV Nutzsignal übertragen hin- bzw. herübertragen wird, wobei auf die zu übertragende Information auf die beiden Kanäle so verteilt ist, daß sie nur wechselweise und auch nur stufenweise in jeweiliger Kenntnis entschlüsselt werden kann.

Zusammenfassung

Decoder-Einrichtung mit einer Bedienungseinheit, für die Entschlüsselung von verschlüsselten Fernseh-Programmen, mit einem Eingang zum Einspeisen eines verschlüsselten Fernseh-Programmes, einer Entschlüsselungseinrichtung, die ein verschlüsseltes Fernseh-Programm in ein mittels eines Fernseh-Empfängers wiedergebbares Format entschlüsselt, einem Ausgang, der mit einem Fernseh-Empfänger verbindbar ist, um das entschlüsselte Fernseh-Programm in den Fernseh-Empfänger zur Wiedergabe einzuspeisen, einer Schnittstelle für ein Identifikations- und/oder Schlüsselträgerbauteil zur Freigabe des Entschlüsselungseinrichtung, und einer Schnittstelle für eine Bedienungseinheit der Decoder-Einrichtung, wobei die Schnittstelle für das Identifikations- und/oder Schlüsselträgerbauteil in der Bedienungseinheit der Decoder-Einrichtung angeordnet ist.

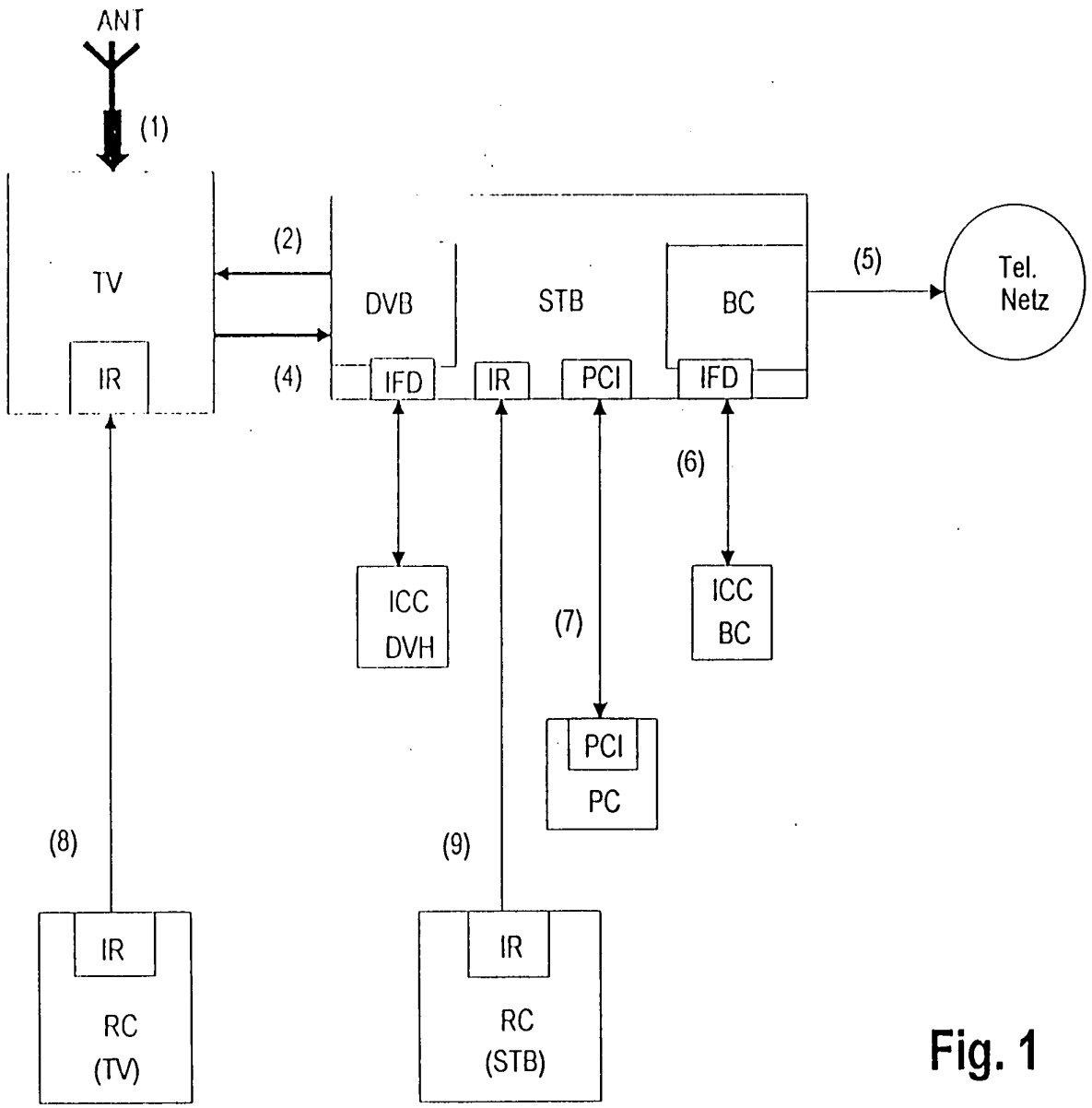
ANT
(1)
TV
IR
(2)
(4)
DVB
IFD
STB
IR
PCI
BC
IFD
(5)
Tel.
Netz
(6)
ICC
DVH
(7)
ICC
BC
PCI
PC
(8)
IR
RC
(TV)
(9)
IR
RC
(STB)

Fig. 1

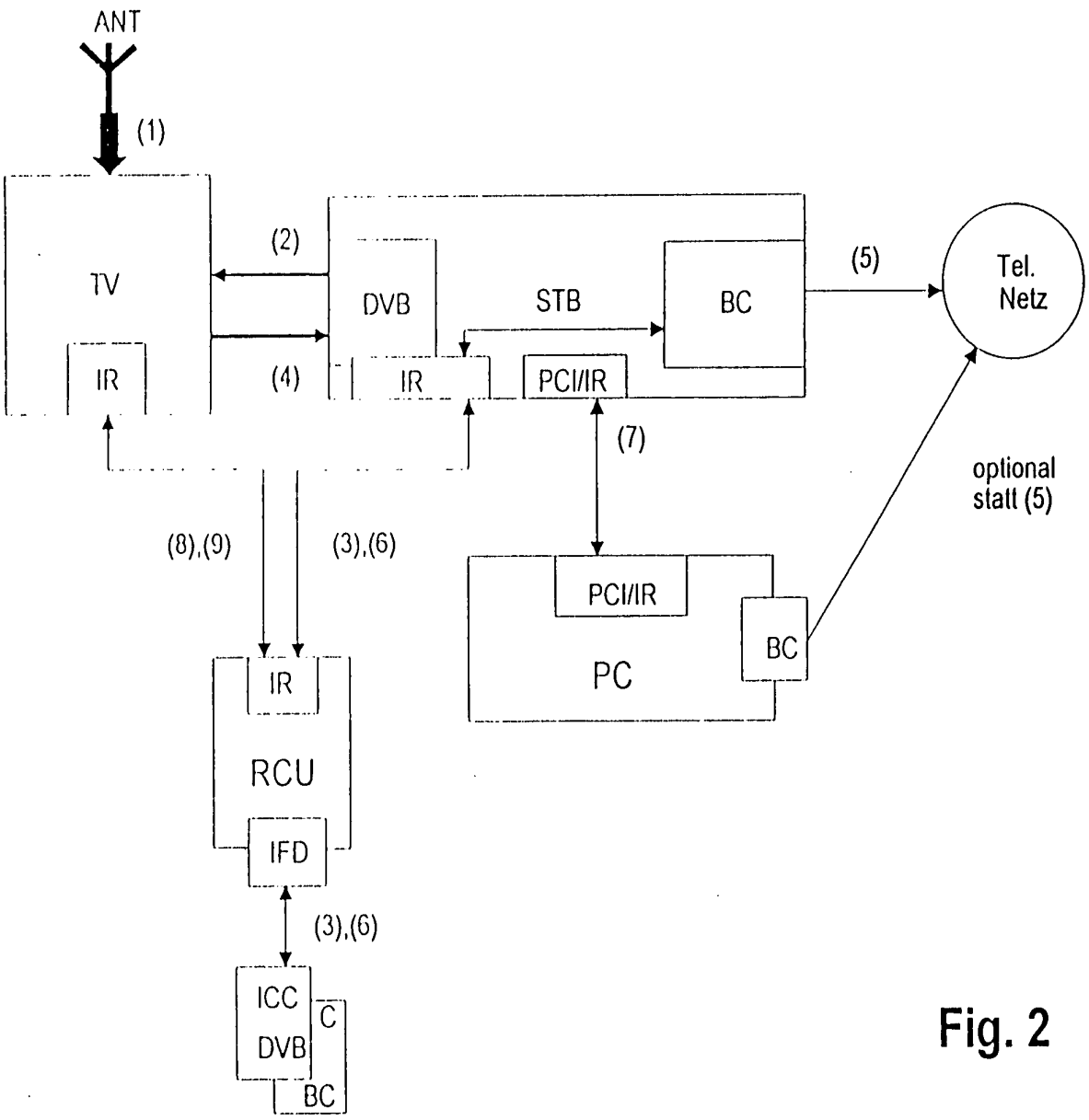
ANT
(1)
TV
IR
(2)
(4)
DVB
IR
STB
BC
PCI/IR
(5)
Tel.
Netz
(7)
optional
statt (5)
(8),(9)
(3),(6)
PCI/IR
BC
PC
IR
RCU
IFD
(3),(6)
ICC
DVB
C
BC

Fig. 2

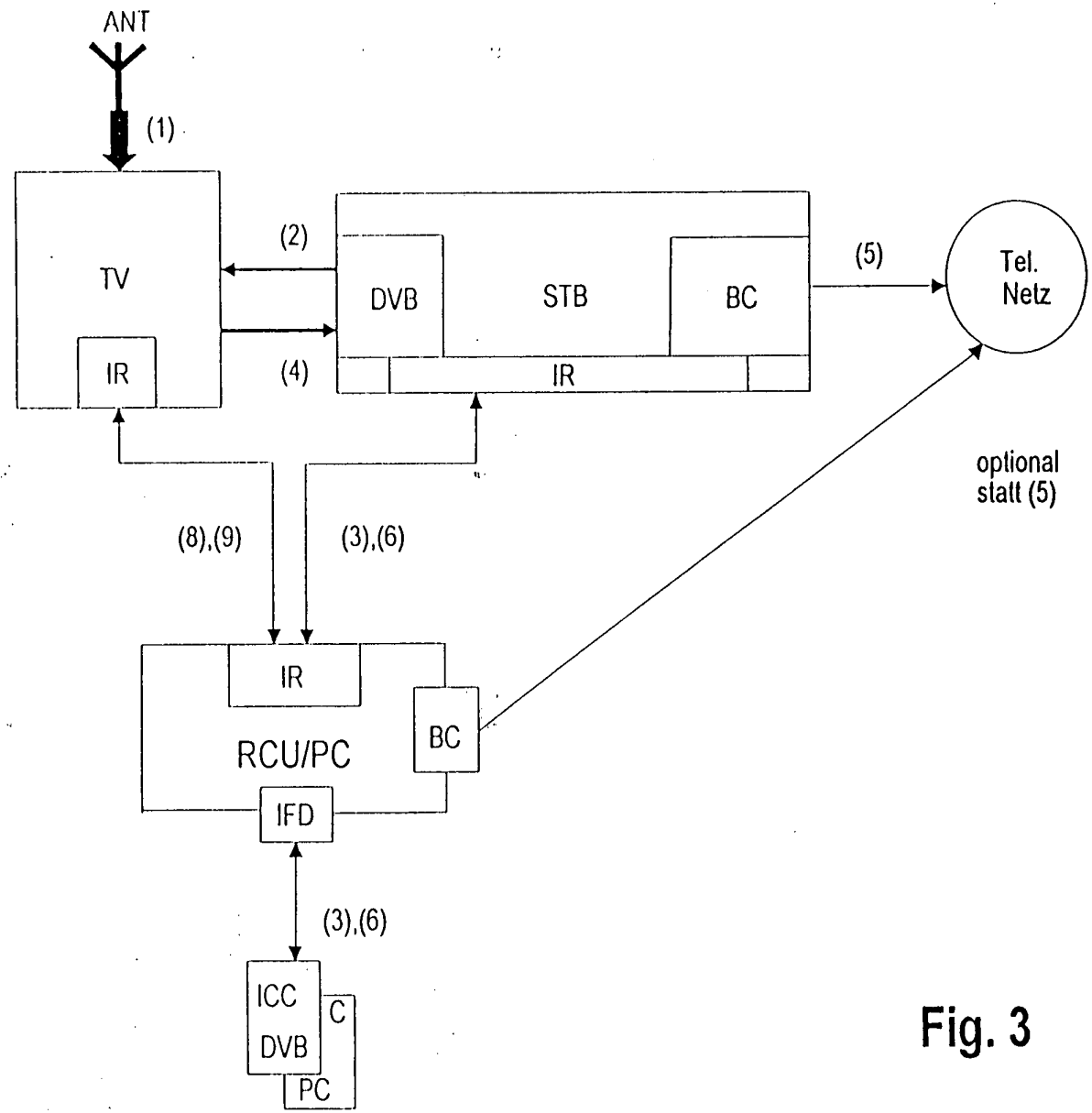
ANT
(1)
TV
IR
(2)
(4)
DVB
STB
BC
IR
(5)
Tel.
Netz
optional
statt (5)
(8),(9)
(3),(6)
IR
RCU/PC
BC
IFD
(3),(6)
ICC
DVB
C
PC

Fig. 3

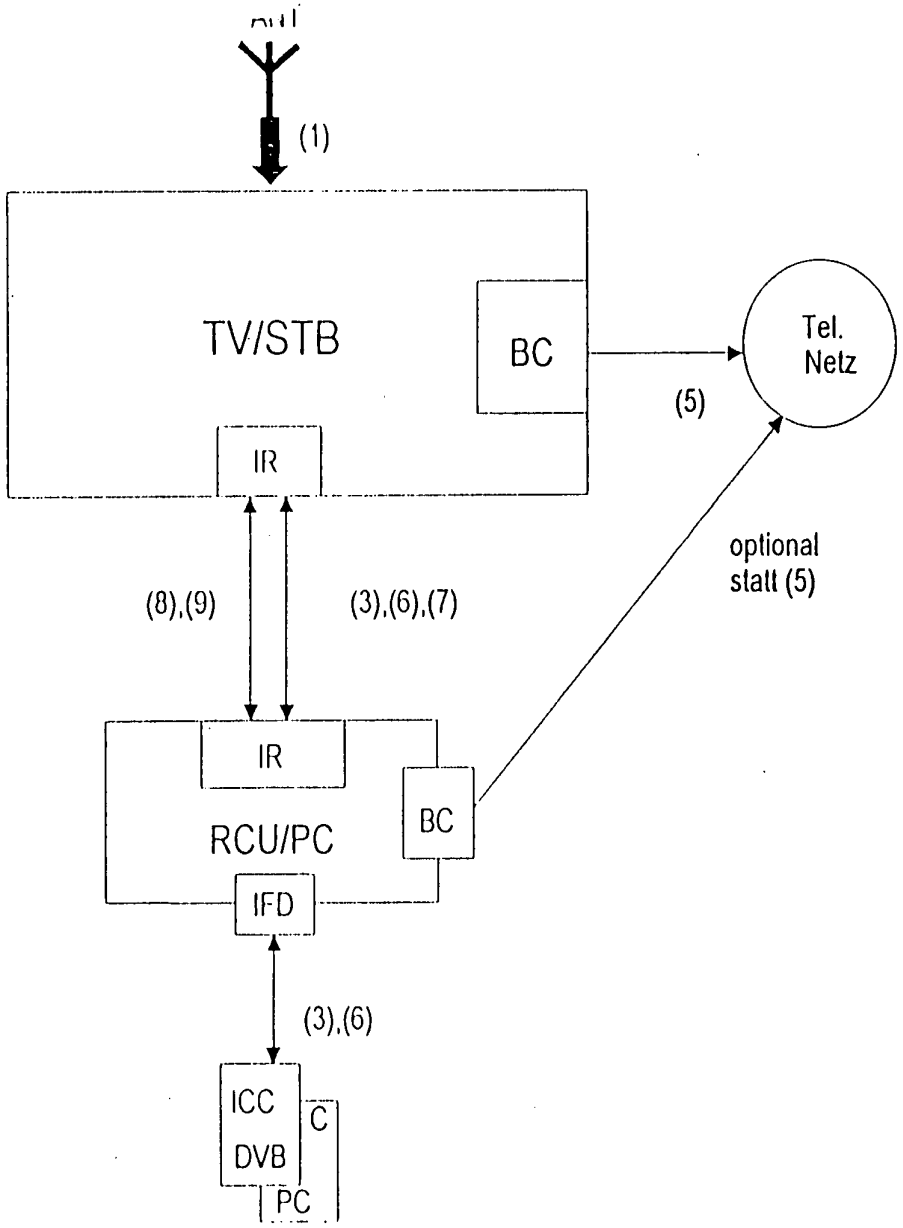
(1)
TV/STB
BC
Tel.
Netz
(5)
IR
optional
statt (5)
(8),(9)
(3),(6),(7)
IR
RCU/PC
BC
IFD
(3),(6)
ICC
DVB
C
PC

Fig. 4